

25

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-047020
(43)Date of publication of application : 12.02.2004

(51)Int.Cl. G11B 5/82
G11B 5/012
G11B 5/73
G11B 20/10
G11B 20/12

(21)Application number :	2002-205886	(71)Applicant : FUJI ELECTRIC HOLDINGS CO LTD
(22)Date of filing :	15.07.2002	(72)Inventor : YUZAWA TAKESHI SATO KIMINORI

(54) MAGNETIC DISK MEDIUM AND FIXED MAGNETIC DISK DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To enable incorporating ID information which is hard to alter and has uniqueness is enabled to embed in a magnetic disk medium.

SOLUTION: ID information for discriminating the media uniquely is divided into master ID information 3 of a pre-format region of a pre-embossed magnetic disk and media individual ID information 4 of a non-pre-format region and they are recorded.

CLAIMS

[Claim(s)]

[Claim 1]

It is the Puri embossing-die magnetic disk medium with which a non-preformatting field which consists of a preformat fielda creviceor heights which consists of uneven parts is established in a record sectionA magnetic disk mediumwherein ID information for identifying this magnetic disk medium uniquely is recorded in said record section and this ID information is further constituted by the 1st ID information in said preformat fieldand the 2nd ID information in said non-preformatting field.

[Claim 2]

In the magnetic disk medium according to claim 1an uneven part which forms said

1st ID information in said preformat fieldA magnetic disk mediumwherein the depth of a crevice is set as sufficient depth which cannot reverse a magnetizing direction by a magnetic field generated from a gap of a recording head of a hard disk drive which builds in said magnetic disk medium.

[Claim 3]

A magnetic disk mediumwherein said 1st and 2nd ID information is recorded for every recording surface of said magnetic disk medium and each information has ID information differentrespectively further in the magnetic disk medium according to claim 1.

[Claim 4]

A magnetic disk medium characterized by said 1st and 2nd ID information being information enciphered by a predetermined cipher system in the magnetic disk medium according to claim 1.

[Claim 5]

The magnetic disk medium comprising according to claim 1:

Said 1st and 2nd ID information is an ID information main part as identification information.

The digital signature information.

[Claim 6]

A hard disk drive which built in one or more sheets of the magnetic disk medium according to claim 1 comprising:

A read-out means for reading said 1st and 2nd ID information of said magnetic disk medium.

A code release means of which a code of said 1st and 2nd ID information is canceled.

A checking means which checks said 1st and 2nd ID information based on digital signature information.

A transfer means which transmits a pair of said 1st and 2nd ID information to an upper device.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

This invention relates to the hard disk drive and magnetic disk medium which carry out record reproduction of the digital information by a magnetic head.

It is related with the hard disk drive which added the security functionand its magnetic disk medium by embedding the identification information of media especially at a magnetic disk medium.

[0002]

[Description of the Prior Art]

The hard disk drive is performing record reproduction of the signal maintaining the interval of a magnetic head's submicron order of on the magnetic disk board rotated at high speed and rising to surface. On the flat substrate made from nonmagnetic material such as aluminum and glass the conventional magnetic disk board used for a hard disk drive laminated the magnetic layer and the protective film and was made. However the magnetic disk of the PURIEMBOSU method which records preformat information including servo data etc. on the uneven pattern provided on the substrate is used for some hard disk drives in recent years.

[0003]

For example the PURIEMBOSU medium which formed the servo pattern and the recording track on the glass substrate with uneven shape is used for the hard disk drive currently introduced to Nikkei electronics No.586 (1993.7.19). A crevice and heights are mutually magnetized for reverse along the track direction and the servo pattern of this medium detected the magnetic flux which leaks and comes out of a concavo-convex boundary part by the magnetic head and has read 1/0 of signal patterns.

[0004]

Since such a PURIEMBOSU method magnetic disk uses the same manufacturing method as an optical disc it is the feature that servo data and a recording track can be formed with sufficient accuracy.

The use to the ROM disk in which this method stored a program data etc.

beforehand for example in addition to the use to a servo pattern is expected.

By the way image data voice data and various software data (these are hereafter called contents) are circulating via network such as the Internet these days. When these contents are purchased and downloaded from a network the hard disk drive and the memory card are used as a means for saving the data temporarily.

[0005]

The digital copyright management system is introduced as structure for protecting contents with increase of the turn volume of digital contents. The digital copyright management system can pass a third party this copy or it is uploaded on the Internet and it prevents from distributing it by performing a certain operation to the contents which the customer purchased.

[0006]

The structure which cannot be reproduced unless a certain kind of digital copyright management system generates a key based on the hardware information of client PC which reproduces contents and has the key is provided. For example the ID information peculiar to a card embedded in the smart card is used for a certain system which cooperated with the smart card (memory card provided with intelligent functions) as hardware information. This ID information is embedded in the state where it cannot alter and thereby has realized high security nature.

[0007]

[Problem(s) to be Solved by the Invention]

On the other hand in the hard disk drive the example which embedded to media ID information which was mentioned above was not seen until now. It is the one Reason that it is that rewriting of a structure top in-house data is comparatively easy for a hard disk drive. That is it is difficult to prevent the alteration of the ID information aiming at an unauthorized use in the method of embedding ID information in soft by a magnetic head.

[0008]

With the Puri embossing-die magnetic disk mentioned above as the solution how to embed ID information in hard can be considered. However in the Puri embossing-die magnetic disk molded by La Stampa there is a problem of having ID information with same magnetic disk molded by the same La Stampa. That is the uniqueness of ID information cannot be maintained.

An object of this invention is to provide the magnetic disk medium which an alteration is difficult and can embed ID information with uniqueness in view of an above-mentioned point and the hard disk drive which added the security function by applying this.

[0009]

[Means for Solving the Problem]

In order to attain the above-mentioned purpose a magnetic disk medium of this invention It is the Puri embossing-die magnetic disk medium with which a non-preformatting field which consists of a preformat field a crevice or heights which consists of uneven parts is established in a record section ID information for identifying this magnetic disk medium uniquely is recorded in said record section and it is characterized by this ID information being further constituted by the 1st ID information in a preformat field and the 2nd ID information in a non-preformatting field.

[0010]

Here ID information which comprises the 1st ID information in a preformat field and the 2nd ID information in a non-preformatting field is difficult to alter and it turns into information which has uniqueness.

An uneven part which forms said 1st ID information in a preformat field in the above-mentioned magnetic disk medium It is preferred that the depth of a crevice is set as sufficient depth which cannot reverse a magnetizing direction by a magnetic field generated from a gap of a recording head of a hard disk drive which builds in said magnetic disk medium. It becomes impossible to rewrite a crevice at least by a head of a hard disk drive now. That is it becomes difficult for an unauthorized use person to change master ID information into contents which he means.

[0011]

As for said 1st and 2nd ID information in the above-mentioned magnetic disk medium it is preferred that it is recorded for every recording surface of said magnetic disk medium and each information has ID information different respectively further. Since two or more ID information becomes available a more flexible

security management becomes possible and the usefulness of this magnetic disk medium can be improved.

[0012]

As for said 1st and 2nd ID information in the above-mentioned magnetic disk medium it is preferred that it is the information enciphered by a predetermined cipher system. Disclosure of ID information by decomposition investigation of a hard disk drive is prevented by encryption.

As for said 1st and 2nd ID information in the above-mentioned magnetic disk medium it is preferred an ID information main part as identification information and to include the digital signature information. Since an unjust alteration of ID information is detected by digital signature information the reliability of ID information can be improved.

[0013]

As for this invention a hard disk drive of this invention is characterized by that a hard disk drive which built in one or more magnetic disk media of this invention comprises the following again in order to attain the above-mentioned purpose. A read-out means for reading said 1st and 2nd ID information of said magnetic disk medium.

A code release means of which a code of said 1st and 2nd ID information is canceled.

A checking means which checks said 1st and 2nd ID information based on digital signature information.

A transfer means which transmits a pair of said 1st and 2nd ID information to an upper device.

[0014]

[Embodiment of the Invention]

Hereafter with reference to Drawings an embodiment of the invention is described in detail.

The composition of the hard disk drive of the embodiment of this invention is shown in drawing 5. As for the hard disk drive 5 the carriage 16 of the shape of a ctenidium which fixes the arm 15 which supports the magnetic head 14 and the arm 15 the voice coil motor 17 which drives this and the magnetic disk 1 are attached on the case 11. The plural laminates of the magnetic disk 1 are carried out and it is being fixed to the spindle shaft 12. The spindle shaft 12 rotates with fixed angular velocity with the spindle motor which is attached to the case 11 bottom and which is not illustrated. The carriage 16 carries out rocking movement a center [the shaft 13] with the voice coil motor 17. The magnetic head 14 is attached at the tip of the arm 15 so that each disc face may be countered and it moves rising to surface the disk top which rotates with movement of the carriage 16.

[0015]

Drawing 2 is a top view of the magnetic disk which is an embodiment of the magnetic disk medium of this invention. A part of recorded information is the Puri embossing-die magnetic disk formed by the uneven part a synthetic resin etc. are

used as a substrate material and as for the magnetic disk 1 the magnetic film and the protective film are laminated on it. The track of the concentric circle shape for the servo zone 2 where control information was recorded being radiately established in the recording surface of this magnetic disk 1 and recording data is formed.

[0016]

Drawing 6 is a detail view of the recording surface of the magnetic disk 1. In the field which gave the dot pattern in the figure heights turn into an uneven part and the white portion has become a crevice and except it.

The lattice pattern 23 for detecting track ID 26 for pinpointing a track position and the position gap from the track center of the position of a head and other control information are formed in the servo zone 2 by unevenness.

[0017]

The track is constructed in a form which is divided by the servo zone 2. The guard band 28 for preventing the interference from an adjacent track is formed between tracks of the crevice. There are what was formed only by heights and a thing formed by the uneven part in a track. The track formed only by heights for example track 27 grade is a track (that is reading and writing of data are possible) which is not preformatted and the track 29 formed by the uneven part is a preformatted track (only for reproduction).

[0018]

The preformat and the format with both logical non-preformatting tracks are given. That is it is divided into the sector which is a basic unit of reading and writing. The redundant byte for a data body header information and error corrections in each sector is ***** (ed). The address information of the sector the synchronization information for generating the clock in sync with data etc. are included in header information. The data body is changed into the sign format (for example 2-7 RLL code etc.) which restricted the number of continuous 0.

[0019]

The magnetic disk 1 mentioned above can be manufactured using the manufacturing method of an optical disc. Drawing 4 shows the procedure. The flat state where the glass disc 90 is ground first and there is no crack is made. And the sensitizing agent (resist) 91 is applied on it. And it glares being intermittent according to the pattern which records a laser beam with a laser cutting device. If this is developed the portion with which the laser beam was irradiated will melt and as for it the hollow according to a pattern will be made on the surface. Furthermore nickel is thickly plated on the surface and La Stampa 94 is molded. Furthermore La Stampa 94 is used as a mold the injection molding of the synthetic resin material is carried out and the substrate 95 is molded. A magnetic disk will be completed if a magnetic layer and a protective film are finally laminated by weld slag etc. on the surface of the substrate 95.

[0020]

Furthermore this magnetic disk becomes detectable [a signal pattern] in a magnetic head by performing operation of magnetization. Magnetization magnetizes

to one way which the concavo-convex upper part and the lower part have by the magnetic head which generates a strong magnetic field first as shown in drawing 1 (a) (primary magnetization) and it is magnetized to an opposite direction by the magnetic head which generates a proper magnetic field weaker than primary magnetization like drawing 1 (b) after that (secondary magnetization). In secondary magnetization since it is not reversed magnetization transition comes to generate a crevice on the boundary of an uneven part.

[0021]

Since the voltage signal which has positive or a negative peak according to a magnetization transition direction in the portion of magnetization transition occurs when passing this uneven part while a magnetic head surface a signal pattern can be read if this voltage signal is amplified and peak detection is carried out.

As shown in drawing 3 two kinds of ID information (master ID information 3 and media individual ID information 4) are recorded on the recording surface of this magnetic disk by the predetermined track position and thereby media can be uniquely identified now.

[0022]

Master ID information 3 is embedded beforehand at La Stampa and is transferred by the magnetic disk as an uneven pattern from La Stampa at a molding process. Therefore the magnetic disk molded by the same La Stampa has the same master ID information. Master ID information 3 contains master ID for identifying La Stampa uniquely. Master ID can use the serial number of La Stampa etc. Different master ID information for every recording surface can also be created by molding the recording surface of the rear surface of a magnetic disk using La Stampa of two sheets which embedded different master ID information.

[0023]

Enciphering is preferred when embedding master ID information 3 as an uneven pattern at La Stampa. Thereby the analysis by decomposition investigation of a hard disk drive becomes still more difficult. As a cipher system to be used there are no restrictions in particular in this case.

It is desirable to include the digital signature information on master ID in master ID information 3. This digital signature enables it to verify whether whether master ID's being created by the regular manufacturer and its master ID are altered.

[0024]

This digital signature can be created by enciphering a hash code using the secret key in a public-key crypto system after changing master ID into fixed length data (hash code) by a hash function. When checking this master ID and a digital signature are first read from a magnetic disk encryption release of the digital signature is carried out by the public key which makes the pair of the above-mentioned secret key and a hash code is obtained. And coincidence/disagreement is judged as compared with the hash code which asked for this hash code by the hash function from master ID. If in agreement as a result of a judgment it will be created by the manufacturer with regular master ID and it is presumed that the alteration is not performed.

[0025]

This master ID information 3 is embedded on the preformatted track (track 29 only for reproduction) which consists of an uneven part shown in drawing 6. The track 29 only for this playback can be established in the arbitrary track positions in the magnetic disk 1.

As for the depth of a crevice in the uneven shape of the track 29 only for reproduction it is preferred that the recording magnetic field generated from the gap part of the recording head of a hard disk drive sets it as the depth which does not fully reach a crevice. The optimum value changes by the characteristic the head flying height etc. of a head to be used. Therefore the depth of a crevice chooses an optimum value according to the hard specification of a hard disk drive.

[0026]

Drawing 7 shows the composition of the manufacturing installation 31 used in the process in which La Stampa which embedded master ID is manufactured. This device is used in order to write the pattern according to unevenness in the surface of the glass substrate which applied resist. Next operation of this manufacturing installation is explained.

First the master ID generating machine 32 generates a meaning ID number for example 10572972 and the encryption machine 33 enciphers this with the common key 96 inputted from the outside. The hash function computing unit 34 changes into 128 bytes of fixed-length hash code master ID enciphered by the predetermined hash function operation. Furthermore the encryption machine 35 enciphers this hash code with the secret key 97 inputted from the outside and creates the digital signature 36.

[0027]

It is combined and master ID 37 and the digital signature 36 which were enciphered are inputted into the format converter 38. The format converter 38 changes byte format input data into a serial bit sequence and performs format conversion according to the logical format of a track and performs conversion to a further predetermined sign format. Furthermore the mapping computing unit 39 maps the output data of the format converter 38 to a two-dimensional field based on the track position which records master ID information and generates the uneven pattern information on master ID information.

[0028]

The ZAKA Tyng device 40 inputs the uneven pattern information 39a which the mapping computing unit 39 generated as the master data 41 which stored the uneven pattern information on a servo zone or a recording track. And the laser 42 is turned on and off based on these input rotating the glass substrate 90 which applied the photo conductor to the surface. Furthermore this glass substrate 90 is developed and La Stampa is completed by performing nickel plate processing to the unevenness formed in that surface.

[0029]

Since master ID information is difficult to change into arbitrary information by a magnetic head as mentioned above there is an advantage of excelling in the

Tampa-proof nature. On the other hand since it will have ID information with same magnetic disk manufactured from the same La Stamp there is a fault that uniqueness cannot be maintained. In order to compensate this fault media individual ID information is used for the magnetic disk of this invention as the 2nd ID information. Media individual ID information contains the ID number which identifies a magnetic disk uniquely.

[0030]

Media individual ID information which is different in the recording surface of the rear surface of a magnetic disk is recordable. Since two or more ID information becomes available with the magnetic disk of one sheet by this a more flexible security management becomes possible.

When writing this ID information as well as master ID information in a magnetic disk it is desirable to perform cipher processing. There are no restrictions in particular in the cipher system similarly used also in this case. It is desirable to include digital signature information also in media individual ID information like master ID information.

[0031]

This media individual ID information is recorded on the track except the track 29 only for reproduction of drawing 6 i.e. the track which is not preformatted (track 27 grade) by a magnetic head. There are no restrictions in particular in a track position here. Processing which records this ID information in a manufacturing process is performed after all assemblies of a hard disk drive are completed.

[0032]

Drawing 9 shows the composition of the device which writes in individual media ID information to the magnetic disk 1 built in the hard disk drive 5. As shown in a figure writing connects by bus 62 and performs the ID write in device 70 and the hard disk drive 5.

In a figure the ID write in device 70 enciphers ID number 71a peculiar to media which the media individual ID generating machine 71 generates with the encryption machine 72 and create the code data 79 and. The hash function computing unit 73 and the encryption machine 74 generate the digital signature 78 and the right data 82 with which these were doubled are created. Media individual ID information 4 is written in the predetermined recording surface of the predetermined track of the magnetic disk 1 by sending a track number and the head number 77 to the hard disk drive 5 as instructions of writing with the right data 82.

[0033]

Drawing 8 is a lineblock diagram of the control section 50 of the hard disk drive of the embodiment of this invention. The head amplifier 51 of this control section 50 comprises read amplifier (figure abbreviation) which amplifies a head regenerative signal a driver circuit (figure abbreviation) which switches the recording current of the magnetic head 14a head selection circuitry (figure abbreviation) etc. The output signal of the head amplifier 51 is led to the read-out control section 53 and reproduction of data is performed here. The read-out control section 53 includes the peak detection circuit 53a which performs peak detection of a regenerative

signal the demodulator circuit 53b which performs decryption of data by which channel coding was carried out etc. The format control part 56 performs format conversion of a lead/right data based on a predetermined sector format check of the lead data based on an error correcting code correction processing at the time of error generating etc. The buffer memory 63 is a memory for storing temporarily the data which carries out read/write.

[0034]

This hard disk drive is connected with the upper device 61 (for example PC) via the bus 62. CPU 58 analyzes the command sent from the upper device 61 and performs processing of each command.

ROM 58a is the read-only memory which memorized the firmware of this device.

The key table 101 which kept some key data which is needed when reading ID information to ROM 58a further is memorized. Drawing 11 shows the contents of the key table 101. The key as the common key 96 inputted into the encryption machine 33 in the La Stampa manufacturing installation of drawing 7 with the same common key 101a for master ID and the public key 101b for master ID are the secret key 97 inputted into the encryption machine 35 and a public key which makes a pair. The key as the common key 98 inputted into the encryption machine 72 in the ID information record measure 70 of drawing 9 with the same common key 101c for media individual ID and 101 d of public keys for media individual ID are the secret key 99 inputted into the encryption machine 74 and a public key which makes a pair.

[0035]

Drawing 10 is the flow chart which showed the procedure in the case of reading the ID information stored in the magnetic disk in the hard disk drive of this invention. The initializing process after powering on was completed and the hard disk drive 5 assumes here that it is a command wait state from the upper device 61. Next the procedure of read-out of ID information is explained to be this flow chart using drawing 8 drawing 11 etc.

[0036]

When read-out instructions of the ID information of a specific head number are sent via the bus 62 from the upper device 61 CPU 58 sends instructions to the positioning control part 54 and makes the head 14 seek in S1 to the track (track only for reproduction) with which master ID information is stored first.

In S2 CPU 58 chooses the head which sent instructions to the head amplifier 51 and the upper device 61 specified as it out of two or more heads. Then the regenerative signal from the recording surface corresponding to the head is amplified with the head amplifier 51 the output is led to the demodulator circuit 53b via the peak detection circuit 53a and the data of the track only for reproduction is read from the demodulator circuit 53b as an NRZ-data sequence.

[0037]

In S3 CPU 58 directs read-out of master ID information in the format control part 56. Then an NRZ-data sequence is inputted into the format control part 56 and only the data of a sector in which master ID information was stored here is

extractedFurthermore the error check of this sector data and an error correction as occasion demands are performed by the format control part 56and sector data is saved via the transfer control circuit 57 at the buffer memory 63 after that.

[0038]

In S4CPU58 accesses the buffer memory 63 firstis stored in the key table 101 and carries out encryption release of the digital signature data in sector data using the public key 101b for master ID. Nextthe hash code of the master ID information in sector data is calculated by a predetermined hash function. The predetermined hash function is a function applied to the hash function computing unit 34 in the La Stampa manufacturing installation of drawing 7and the same function here.

[0039]

In S5CPU58 compares the code which carried out encryption release of the digital signature in a front step with the hash code calculated from master ID. When it carries out also here and these differit judges that media have a certain abnormalitiesand generating of abnormalities is notified to an upper device (S14). And processing is interrupted and it returns to a command wait state (S13).

[0040]

When that is not rightit progresses to the following step S6. In S6CPU58 carries out encryption release with the enciphered common key 101a for master ID. And plaintext-ized master ID (16 bits) is acquired.

NextCPU58 makes the magnetic head 14 seek in S7 to the track with which media individual ID information is stored.

[0041]

Furthermore in S8read-out of the ID information recorded on this track is performedand sector data including media individual ID information is read into the buffer memory 63.

In S9CPU58 carries out encryption release of the digital signature data in sector data first using 101 d of public keys for media individual ID. Nextthe hash code of the data of media individual ID in sector data is calculated by a predetermined hash function. The predetermined hash function is a function applied to the hash function computing unit 73 in the ID information recorder of drawing 9and the same function here.

[0042]

Nextin S9CPU58 compares the code which carried out encryption release of the digital signature in a front step with the hash code calculated from media individual ID. When it carries out also here and these differit judges that media have a certain abnormalitiesand generating of abnormalities is notified to an upper device by S14. And processing is interrupted and it returns to a command wait state.

[0043]

When that is not rightit progresses to the following step S11. In S11CPU58 carries out encryption release of enciphered media individual ID with the common key 101c for media individual ID. And plaintext-ized media individual ID (32 bits) is acquired. Finallyin S12CPU58 combines master ID (16 bits) and media individual ID (32 bits)and creates 48-bit ID. And this is sent to the upper device 61 via the bus

62. And it returns to the command wait state from the upper device 61 by S13 after that.

[0044]

The upper device 61 sends the read-out command of ID similarly to other heads if needed after that. And ID corresponding to each head is acquired and generation of an encryption key etc. are performed based on these.

[0045]

[Effect of the Invention]

According to the magnetic disk medium of this invention dividing the ID information for identifying media uniquely into the preformat field and the non-preformatting field of the Puri embossing-die magnetic disk and having recorded it as explained above, an alteration is difficult and offer of the magnetic disk medium which recorded ID information with uniqueness is attained.

[0046]

Since according to the hard disk drive of this invention the one or more above-mentioned magnetic disk media can be built in, ID information can be read from this magnetic disk medium and it can transmit to an upper device, offer of a hard disk drive applicable to various security systems is attained.

[Brief Description of the Drawings]

[Drawing 1] In the principle explanatory view of initial magnetization of the magnetic disk of the embodiment of this invention (a) shows primary magnetization and (b) shows secondary magnetization in it.

[Drawing 2] It is a top view (the 1) of the magnetic disk of the embodiment of this invention.

[Drawing 3] It is a top view (the 2) of the magnetic disk of the embodiment of this invention.

[Drawing 4] It is an explanatory view of the manufacturing method of the magnetic disk of the embodiment of this invention.

[Drawing 5] It is a lineblock diagram of the hard disk drive of the embodiment of this invention.

[Drawing 6] It is a detail view of the recording surface of the magnetic disk of the embodiment of this invention.

[Drawing 7] It is an explanatory view of the manufacturing installation of La Stampa used for manufacture of the magnetic disk of the embodiment of this invention.

[Drawing 8] It is a lineblock diagram of the control section of the hard disk drive of the embodiment of this invention.

[Drawing 9] It is a lineblock diagram of the write in device of the media individual information of the magnetic disk of the embodiment of this invention.

[Drawing 10] It is a flow chart which shows the procedure which reads the ID information stored in the magnetic disk in the hard disk drive of the embodiment of this invention.

[Drawing 11] It is a figure showing the contents of the key table kept to the hard disk drive of the embodiment of this invention.

[Description of Notations]

1 Magnetic disk

2 Servo zone

3 Master ID information

4 Media individual ID information

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-47020

(P2004-47020A)

(43) 公開日 平成16年2月12日(2004.2.12)

(51) Int.Cl. ⁷	F 1	テーマコード (参考)
G 1 1 B 5/82	G 1 1 B 5/82	5 D 0 0 6
G 1 1 B 5/012	G 1 1 B 5/012	5 D 0 4 4
G 1 1 B 5/73	G 1 1 B 5/73	5 D 0 9 1
G 1 1 B 20/10	G 1 1 B 20/10	H
G 1 1 B 20/12	G 1 1 B 20/12	
審査請求 未請求 請求項の数 6 O L (全 12 頁)		
(21) 出願番号	特願2002-205886 (P2002-205886)	(71) 出願人 000005234 富士電機ホールディングス株式会社 神奈川県川崎市川崎区田辺新田 1 番 1 号
(22) 出願日	平成14年7月15日 (2002.7.15)	(74) 代理人 100088339 弁理士 篠部 正治 (72) 発明者 由沢 剛 神奈川県川崎市川崎区田辺新田 1 番 1 号 富士電機株式会社内 (72) 発明者 佐藤 公紀 神奈川県川崎市川崎区田辺新田 1 番 1 号 富士電機株式会社内
		F ターム (参考) 5D006 BB07 CB07 DA03 EA03 FA00 5D044 AB01 BC01 CC05 DE49 DE53 CK17 HH13 HH15 5D091 AA10 BB02 BB04 CC01 DD01 GG40 HH01 HH04

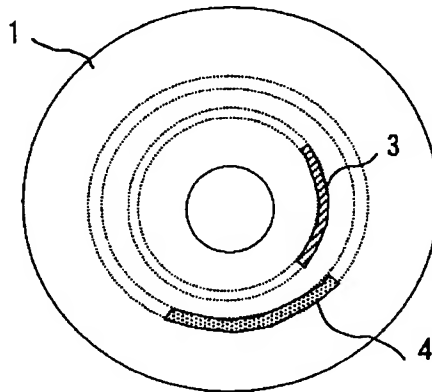
(54) 【発明の名称】 磁気ディスク媒体及び固定磁気ディスク装置

(57) 【要約】

【課題】改竄が困難であると共に、一意性の有る I D 情報を磁気ディスク媒体に埋め込むことを可能とする。

【解決手段】メディアを一意に識別するための I D 情報を、プリエンボス型磁気ディスクのプリフォーマット領域のマスタ I D 情報 3 と、非プリフォーマット領域のメディア個別 I D 情報 4 とに分けて記録する。

【選択図】 図 3



【特許請求の範囲】

【請求項 1】

記録領域に凹凸部からなるプリフォーマット領域と凹部又は凸部からなる非プリフォーマット領域が設けられているプリエンボス型磁気ディスク媒体であって、該磁気ディスク媒体を一意に識別するための I D 情報が前記記録領域内に記録されており、さらに該 I D 情報が前記プリフォーマット領域内の第 1 の I D 情報と、前記非プリフォーマット領域内の第 2 の I D 情報により構成されていることを特徴とする磁気ディスク媒体。

【請求項 2】

請求項 1 に記載の磁気ディスク媒体において、前記プリフォーマット領域において前記第 1 の I D 情報を形成する凹凸部は、凹部の深さが前記磁気ディスク媒体を内蔵する固定磁気ディスク装置の記録ヘッドのギャップから発生する磁界により磁化方向を反転不能な十分な深さに設定されていることを特徴とする磁気ディスク媒体。

10

【請求項 3】

請求項 1 に記載の磁気ディスク媒体において、前記第 1、第 2 の I D 情報は、前記磁気ディスク媒体の記録面毎に記録され、さらに各情報がそれぞれ異なる I D 情報を有することを特徴とする磁気ディスク媒体。

【請求項 4】

請求項 1 に記載の磁気ディスク媒体において、前記第 1 及び第 2 の I D 情報は、所定の暗号方式により暗号化された情報であることを特徴とする磁気ディスク媒体。

20

【請求項 5】

請求項 1 に記載の磁気ディスク媒体において、前記第 1、第 2 の I D 情報は、識別情報としての I D 情報本体と、そのデジタル署名情報を含むことを特徴とする磁気ディスク媒体。

30

【請求項 6】

請求項 1 に記載の磁気ディスク媒体を 1 枚以上内蔵した固定磁気ディスク装置であって、前記磁気ディスク媒体の前記第 1、第 2 の I D 情報を読み出すための読出し手段と、前記第 1、第 2 の I D 情報の暗号を解除する暗号解除手段と、前記第 1、第 2 の I D 情報をデジタル署名情報に基づきチェックするチェック手段と、前記第 1、第 2 の I D 情報のペーアを上位装置に転送する転送手段とを備えることを特徴とする固定磁気ディスク装置。

【発明の詳細な説明】

40

【0001】

【発明の属する技術分野】

本発明は、磁気ヘッドによりデジタル情報を記録再生する固定磁気ディスク装置と磁気ディスク媒体に関するものであり、特に磁気ディスク媒体にメディアの識別情報を埋め込むことによりセキュリティ機能を加えた固定磁気ディスク装置とその磁気ディスク媒体に関する。

【0002】

【従来の技術】

固定磁気ディスク装置は高速で回転する磁気ディスク基板上を磁気ヘッドがサブミクロンオーダーの間隔を保って浮上しながら、信号の記録再生を行っている。固定磁気ディスク装置に用いられる従来の磁気ディスク基板は、アルミやガラス等の非磁性体を材料とする平坦な基板上に、磁性層と保護膜を積層して作られていた。ところが近年、基板上に設けられた凹凸パターンにサーボ情報等のプリフォーマット情報を記録するプリエンボス方式の磁気ディスクが一部の固定磁気ディスク装置に用いられるようになってきている。

40

【0003】

例えば日経エレクトロニクス No. 586 (1993. 7. 19) に紹介されている固定磁気ディスク装置は、サーボパターンと記録トラックを凹凸形状でガラス基板上に形成したプリエンボス媒体を用いている。本媒体のサーボパターンは凹部と凸部がトラック方向に沿って互いに逆向きに磁化されており、凹凸の境界部分から漏れ出る磁束を磁気ヘッドで検出し、1/0 の信号パターンを読み取っている。

50

【0004】

このようなプリエンボス方式磁気ディスクは光ディスクと同様の製造方法を用いるので、サーボ情報や記録トラックを精度良く形成できるのが特徴である。

なお、本方式はサーボパターンへの用途以外に、例えばプログラムやデータ等をあらかじめ格納したROMディスクへの用途が期待されている。

ところで昨今、画像データ、音声データ、様々なソフトウェアデータ（以下、これらをコンテンツと呼ぶ）が、インターネット等のネットワークを介して流通している。これらのコンテンツをネットから購入、ダウンロードした際にそのデータを一時的に保存するための手段として固定磁気ディスク装置やメモリカードが用いられている。

【0005】

また、デジタルコンテンツの流通量の増大に伴い、コンテンツを保護するための仕組みとしてデジタル著作権管理システムが導入されている。デジタル著作権管理システムは、顧客が購入したコンテンツに何らかの操作を施すことで、このコピーを第三者に渡したり、インターネットにアップロードして配布したりすることができないようにするものである。

【0006】

ある種のデジタル著作権管理システムは、コンテンツを再生するクライアントPCのハードウェア情報をベースにキーを生成して、そのキーが無いと再生できないような仕組みを提供している。例えばスマートカード（インテリジェント機能を備えるメモリカード）と連携した或るシステムは、ハードウェア情報としてスマートカード内に埋め込まれたカード固有のID情報を用いる。このID情報は改竄できないような状態で埋め込まれており、これにより高いセキュリティ性を実現している。

【0007】

【発明が解決しようとする課題】

一方、固定磁気ディスク装置において、上述したようなID情報をメディアに埋め込んだ例はこれまで見られなかった。固定磁気ディスク装置は構造上内部データの書き換えが比較的容易なことなどがその一つの理由となっている。すなわちID情報を磁気ヘッドでソフト的に埋め込む方法では、不正使用を目的とするID情報の改竄を防ぐことが難しい。

【0008】

その解決策として上述したプリエンボス型磁気ディスクにより、ID情報をハード的に埋め込む方法が考えられる。しかしスタンパで成型するプリエンボス型磁気ディスクでは、同一スタンパで成型した磁気ディスクが同一のID情報を有するという問題がある。すなわちID情報の一意性を保つことができない。

本発明は、上述の点に鑑み、改竄が困難であると共に、一意性の有るID情報を埋め込むことが可能な磁気ディスク媒体と、これを適用することでセキュリティ機能を付加した固定磁気ディスク装置とを提供することを目的とする。

【0009】

【課題を解決するための手段】

上述の目的を達成するため、本発明の磁気ディスク媒体は、記録領域に凹凸部からなるプリフォーマット領域と凹部又は凸部からなる非プリフォーマット領域が設けられているプリエンボス型磁気ディスク媒体であって、該磁気ディスク媒体を一意に識別するためのID情報が前記記録領域内に記録されており、さらに該ID情報がプリフォーマット領域内の第1のID情報と、非プリフォーマット領域内の第2のID情報により構成されていることを特徴としている。

【0010】

ここで、プリフォーマット領域内の第1のID情報と非プリフォーマット領域内の第2のID情報から構成されるID情報は、改竄が困難であると共に一意性を有する情報となる。

また、上記磁気ディスク媒体において、プリフォーマット領域内の前記第1のID情報を

10

20

30

40

50

形成する凹凸部は、凹部の深さが前記磁気ディスク媒体を内蔵する固定磁気ディスク装置の記録ヘッドのギャップから発生する磁界により磁化方向を反転不能な十分な深さに設定されていることが好ましい。これで固定磁気ディスク装置のヘッドにより、少なくとも凹部を書き換えることができなくなる。すなわち不正使用者がマスタID情報を自分の意図する内容に変更することが困難になる。

【0011】

また、上記磁気ディスク媒体において、前記第1、第2のID情報は、前記磁気ディスク媒体の記録面毎に記録され、さらに各情報がそれぞれ異なるID情報を有することが好ましい。複数のID情報が利用可能となるため、より柔軟なセキュリティ管理が可能となり、本磁気ディスク媒体の有用性を高めることができる。

10

【0012】

また、上記磁気ディスク媒体において、前記第1及び第2のID情報は、所定の暗号方式により暗号化された情報であることが好ましい。暗号化により固定磁気ディスク装置の分解調査によるID情報の漏洩が防止される。

また、上記磁気ディスク媒体において、前記第1、第2のID情報は、識別情報としてのID情報本体と、そのデジタル署名情報を含むことが好ましい。デジタル署名情報によりID情報の不正な改竄が検知されるため、ID情報の信頼性を高めることができる。

【0013】

また、本発明の固定磁気ディスク装置は、上述の目的を達成するため、本発明の磁気ディスク媒体を1枚以上内蔵した固定磁気ディスク装置において、前記磁気ディスク媒体の前記第1、第2のID情報を読み出すための読出し手段と、前記第1、第2のID情報の暗号を解除する暗号解除手段と、前記第1、第2のID情報をデジタル署名情報に基づきチェックするチェック手段と、前記第1、第2のID情報のペアを上位装置に転送する転送手段とを備えることを特徴とする。

20

【0014】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の形態を詳細に説明する。

図5に本発明の実施形態の固定磁気ディスク装置の構成を示す。固定磁気ディスク装置5は、筐体11の上に磁気ヘッド14を支持するアーム15、アーム15を固定する櫛歯状のキャリッジ16、及びこれを駆動するボイスコイルモータ17、及び磁気ディスク1が取り付けられている。磁気ディスク1は複数積層されてスピンドル軸12に固定されている。スピンドル軸12は筐体11の下側に取り付けられている図示しないスピンドルモータにより一定の角速度で回転する。キャリッジ16はボイスコイルモータ17によりシャフト13を中心に揺動運動する。磁気ヘッド14は各ディスク面に対向するようにアーム15の先端に取り付けられ、キャリッジ16の移動に伴って回転するディスク上を浮上しながら移動するようになっている。

30

【0015】

図2は本発明の磁気ディスク媒体の実施形態である磁気ディスクの平面図である。磁気ディスク1は記録情報の一部が凹凸部で形成されたプリエンボス型磁気ディスクであり、基板材料として合成樹脂等が使用され、その上に磁性膜と保護膜が積層されている。本磁気ディスク1の記録面には制御情報が記録されたサーボゾーン2が放射状に設けられており、またデータを記録するための同心円状のトラックが設けられている。

40

【0016】

図6は磁気ディスク1の記録面の詳細図である。図においてドット模様を施した領域は凸部、白抜き部分は凹部、それ以外は凹凸部となっている。

サーボゾーン2には、トラック位置を特定するためのトラックID26、及びヘッドの位置のトラック中心からの位置ずれを検知するための格子パターン23、及びその他の制御情報が凹凸で形成されている。

【0017】

サーボゾーン2により分割されるような形でトラックが敷設されている。また隣接トラッ

50

クからの干渉を防止するためのガードバンド 28 が凹部によりトラック間に形成されている。トラックには凸部のみで形成されたものと、凹凸部で形成されたものがある。凸部のみで形成されたトラック、例えばトラック 27 等はプリフォーマットされていない（すなわちデータの読み書きが可能な）トラックであり、凹凸部で形成されたトラック 29 はプリフォーマットされた（再生専用の）トラックである。

【0018】

プリフォーマット及び非プリフォーマットトラックは共に論理的なフォーマットが施されている。すなわち読み書きの基本単位であるセクタに分割されている。各々のセクタはデータ本体とヘッダ情報、及び誤り訂正用の冗長バイトがから構成されている。ヘッダ情報にはそのセクタのアドレス情報や、データに同期したクロックを生成するための同期情報等が含まれている。またデータ本体は連続する 0 の数を制限した符号形式（例えば 2-7 RLL 符号等）に変換されている。

10

【0019】

上述した磁気ディスク 1 は光ディスクの製造方法を用いて製造することができる。図 4 はその手順を示したものである。まずガラス円盤 90 を研磨してキズの無い、平坦な状態に仕上げる。そしてその上に感光剤（レジスト）91 を塗布する。そしてレーザーカッティング装置にてレーザー光を記録するパターンに応じて断続しながら照射する。これを現像するとレーザー光が照射された部分は溶けて、表面にパターンに応じたくぼみができる。さらにその表面にニッケルを厚くメッキしスタンパ 94 を型取りする。さらにスタンパ 94 を型にして合成樹脂材料を射出成型し、基板 95 を成型する。最後に基板 95 の表面にスパッタ等により磁性層と保護膜を積層すると磁気ディスクが完成する。

20

【0020】

さらに本磁気ディスクは着磁という操作を行うことにより磁気ヘッドにて信号パターンの検出が可能となる。着磁は図 1 (a) に示すようにまず、強い磁界を発生する磁気ヘッドにより凹凸の上部、下部共にある一方向に着磁を行い（一次着磁）、その後図 1 (b) のように一次着磁より弱い適正な磁界を発生する磁気ヘッドにより逆方向に着磁する（二次着磁）。二次着磁では凹部は反転されないため、凹凸部の境界で磁化遷移が発生するようになる。

【0021】

磁気ヘッドが浮上しながらこの凹凸部を通過する際、磁化遷移の部分で磁化遷移方向に応じて正又は負ピークを持つ電圧信号が発生するため、この電圧信号を増幅してピーク検知すれば信号パターンが読み取れる。

30

図 3 に示したように本磁気ディスクの記録面には、所定のトラック位置に 2 種類の ID 情報（マスタ ID 情報 3 及びメディア個別 ID 情報 4）が記録されており、これによりメディアを一意に識別できるようになっている。

【0022】

マスタ ID 情報 3 はあらかじめスタンパに埋め込まれており、成型工程でスタンパから磁気ディスクに凹凸パターンとして転写されるものである。従って同一のスタンパにより成型された磁気ディスクは同一のマスタ ID 情報を有する。マスタ ID 情報 3 はスタンパを一意に識別するためのマスタ ID を含む。マスタ ID は例えばスタンパのシリアル番号等を用いることができる。異なるマスタ ID 情報を埋め込んだ 2 枚のスタンパを用いて、磁気ディスクの表裏の記録面の成型を行うことにより、記録面毎に異なるマスタ ID 情報を作成することもできる。

40

【0023】

マスタ ID 情報 3 をスタンパに凹凸パターンとして埋め込む場合には暗号化を施すことが好ましい。これにより固定磁気ディスク装置の分解調査による解析がさらに困難となる。使用する暗号方式としてはこの場合特に制約は無い。

また、マスタ ID 情報 3 にはマスタ ID のデジタル署名情報が含まれていることが望ましい。このデジタル署名はマスタ ID が正規の製造者により作成されているか否か、及びそのマスタ ID が改竄されているか否かを検証できるようにするものである。

50

【0024】

このデジタル署名は、マスタIDをハッシュ関数により固定長データ（ハッシュコード）に変換した後、公開鍵暗号方式における秘密鍵を使用してハッシュコードを暗号化することにより作成することができる。これをチェックする場合は、まず磁気ディスクからマスタIDとデジタル署名を読み、デジタル署名を上記の秘密鍵の対をなす公開鍵により暗号化解除してハッシュコードを得る。そしてこのハッシュコードをマスタIDからハッシュ関数により求めたハッシュコードと比較し、一致／不一致を判定する。判定の結果一致していればマスタIDが正規の製造者により作成され、かつその改竄は行われていないと推定される。

【0025】

このマスタID情報3は、図6に示す凹凸部からなるプリフォーマットされたトラック（再生専用トラック29）に埋め込まれる。この再生専用トラック29は磁気ディスク1内の任意のトラック位置に設けることができる。

再生専用トラック29の凹凸形状において、凹部の深さは固定磁気ディスク装置の記録ヘッドのギャップ部から発生する記録磁界が凹部に十分に届かない深さに設定することが好ましい。その最適値は使用するヘッドの特性やヘッド浮上量等により変わる。そのため凹部の深さは固定磁気ディスク装置のハード仕様に合わせて最適値を選ぶ。

【0026】

図7はマスタIDを埋め込んだスタンプを製作する過程で用いる製造装置31の構成を示したものである。本装置はレジストを塗布したガラス基板の表面に凹凸に応じたパターンを書き込むために使用される。次に本製造装置の動作について説明する。

まずマスタID発生器32は一意的なID番号、例えば10572972を発生し、暗号化器33は外部から入力される共通鍵96によりこれを暗号化する。ハッシュ関数演算器34は所定のハッシュ関数演算により暗号化されたマスタIDを例えば128バイトの固定長ハッシュコードに変換する。さらに暗号化器35は外部から入力される秘密鍵97によりこのハッシュコードを暗号化しデジタル署名36を作成する。

【0027】

暗号化されたマスタID37とデジタル署名36は結合されフォーマット変換器38に入力される。フォーマット変換器38はバイト形式の入力データをシリアルビット列に変換すると共に、トラックの論理フォーマットに合わせてフォーマット変換を行い、さらに所定の符号形式への変換を行う。さらにマッピング演算器39はフォーマット変換器38の出力データを、マスタID情報を記録するトラック位置に基づいて2次元領域にマッピングし、マスタID情報の凹凸パターン情報を生成する。

【0028】

レーザーカティング装置40はサーボゾーンや記録トラックの凹凸パターン情報を格納したマスタデータ41と、マッピング演算器39の生成した凹凸パターン情報39aを入力する。そして感光体を表面に塗布したガラス基板90を回転させながら、これらの入力情報に基づいてレーザー42のON/OFFを行う。さらにこのガラス基板90を現像し、その表面に形成された凹凸にニッケルメッキ処理を施すことによりスタンプが完成する。

【0029】

マスタID情報は上述したように磁気ヘッドで任意情報に変更することが困難なため、耐タンパ性に優れるという利点がある。しかしその反面、同一のスタンプから製造された磁気ディスクが同一のID情報を有することになるため、一意性が保てないという欠点がある。この欠点を補うため本発明の磁気ディスクは、第2のID情報としてメディア個別ID情報を使用する。メディア個別ID情報は、磁気ディスクを一意的に識別するID番号を含む。

【0030】

磁気ディスクの表裏の記録面に異なるメディア個別ID情報を記録することができる。これにより1枚の磁気ディスクで複数のID情報が利用可能となるため、より柔軟なセキュリティ管理が可能となる。

10

20

30

40

50

また、マスタ I D 情報と同様に本 I D 情報も磁気ディスクに書き込む際に暗号処理を施すことが望ましい。この場合も同様に使用する暗号方式に特に制約は無い。またマスタ I D 情報と同様にメディア個別 I D 情報にもデジタル署名情報が含まれていることが望ましい。

【0031】

このメディア個別 I D 情報は図 6 の再生専用トラック 29 を除くトラック、すなわちプリフォーマットされていないトラック（トラック 27 等）に磁気ヘッドで記録される。ここでトラック位置に特に制約は無い。製造工程において本 I D 情報を記録する処理は固定磁気ディスク装置の組み立てが全て完了した後に行われる。

【0032】

図 9 は固定磁気ディスク装置 5 に内蔵されている磁気ディスク 1 に個別メディア I D 情報を書き込む装置の構成を示したものである。図のように書込みは I D 書込み装置 70 と固定磁気ディスク装置 5 をバス 62 により接続しておこなう。

図において I D 書込み装置 70 はメディア個別 I D 発生器 71 が生成するメディア固有の I D 番号 71a を、暗号化器 72 で暗号化し、暗号データ 79 を作成すると共に、ハッシュ関数演算器 73 と暗号化器 74 によりそのデジタル署名 78 を生成し、これらを合わせたライトデータ 82 を作成する。ライトデータ 82 と共にトラック番号及びヘッド番号 77 を固定磁気ディスク装置 5 に書込みの指令として送ることにより磁気ディスク 1 の所定トラックの所定記録面にメディア個別 I D 情報 4 が書き込まれる。

【0033】

図 8 は本発明の実施形態の固定磁気ディスク装置の制御部 50 の構成図である。本制御部 50 のヘッドアンプ 51 はヘッド再生信号を増幅するリードアンプ（図省略）、磁気ヘッド 14 の記録電流のスイッチングを行うドライバ回路（図省略）、及びヘッド選択回路等（図省略）から構成されている。ヘッドアンプ 51 の出力信号は読出し制御部 53 に導かれ、ここでデータの再生が行われる。読出し制御部 53 は、再生信号のピーク検出を行うピーク検出回路 53a、チャンネル符号化されたデータの復号化を行う復調回路 53b 等を含む。フォーマット制御部 56 は所定のセクタフォーマットに基づくリード／ライトデータのフォーマット変換、誤り訂正符号によるリードデータのチェック、誤り発生時の訂正処理等を行う。バッファメモリ 63 はリード・ライトするデータを一時的に格納するためのメモリである。

【0034】

本固定磁気ディスク装置はバス 62 を介して上位装置 61（例えば PC）と接続されている。CPU 58 は上位装置 61 から送られてくるコマンドを解析し、各コマンドの処理を実行する。

ROM 58a は本装置のファームウェアを記憶したリードオンリーメモリである。ROM 58a にはさらに、I D 情報を読み出す際に必要となる幾つかの鍵データを保管した鍵テーブル 101 が記憶されている。図 11 は鍵テーブル 101 の内容を示したものである。マスタ I D 用共通鍵 101a は、図 7 のスタンパ製造装置において暗号化器 33 に入力される共通鍵 96 と同一の鍵、マスタ I D 用公開鍵 101b は暗号化器 35 に入力される秘密鍵 97 と対をなす公開鍵となっている。またメディア個別 I D 用共通鍵 101c は、図 9 の I D 情報記録装置 70 において暗号化器 72 に入力される共通鍵 98 と同一の鍵、メディア個別 I D 用公開鍵 101d は暗号化器 74 に入力される秘密鍵 99 と対をなす公開鍵である。

【0035】

図 10 は本発明の固定磁気ディスク装置において磁気ディスクに格納された I D 情報を読み出す場合の手順を示したフローチャートである。ここで固定磁気ディスク装置 5 は電源投入後のイニシャライズ処理が完了し、上位装置 61 からのコマンド待ち状態であると仮定している。次に I D 情報の読み出しの手順を本フローチャートと、図 8、図 11 等を用いて説明する。

【0036】

10

20

30

40

50

上位装置 6 1 からバス 6 2 を介して特定のヘッド番号の I D 情報の読出し指令が送られてくると、まず S 1 において C P U 5 8 は位置決め制御部 5 4 に指令を送り、ヘッド 1 4 をマスタ I D 情報が格納されているトラック（再生専用トラック）へシークさせる。

S 2 において、C P U 5 8 はヘッドアンプ 5 1 に指令を送り複数のヘッドの中から上位装置 6 1 が指定したヘッドを選択する。するとそのヘッドに対応する記録面からの再生信号がヘッドアンプ 5 1 で増幅され、その出力がピーク検出回路 5 3 a を介して復調回路 5 3 b へ導かれ、復調回路 5 3 b から再生専用トラックのデータが N R Z データ列として読み出される。

【 0 0 3 7 】

S 3 において、C P U 5 8 はフォーマット制御部 5 6 にマスタ I D 情報の読出しを指示する。すると N R Z データ列はフォーマット制御部 5 6 に入力され、ここでマスタ I D 情報が格納されたセクタのデータのみが抽出され、さらにフォーマット制御部 5 6 により本セクタデータの誤りチェック、必要に応じた誤り訂正が行われ、その後セクタデータが転送制御回路 5 7 を介してバッファメモリ 6 3 に保存される。

10

【 0 0 3 8 】

S 4 において、C P U 5 8 はまずバッファメモリ 6 3 にアクセスし、セクタデータ内のデジタル署名データを鍵テーブル 1 0 1 に格納されてマスタ I D 用公開鍵 1 0 1 b を用いて暗号化解除する。次に所定のハッシュ関数によりセクタデータ内のマスタ I D データのハッシュコードを計算する。ここで所定のハッシュ関数は図 7 のスタンパ製造装置におけるハッシュ関数演算器 3 4 に適用される関数と同一の関数となっている。

20

【 0 0 3 9 】

S 5 において、C P U 5 8 は前ステップにおけるデジタル署名を暗号化解除したコードと、マスタ I D から計算したハッシュコードを比較する。ここでもしこれらが異なっていた場合は、メディアに何らかの異常があると判断し、上位装置へ異常の発生を通知する（S 1 4）。そして処理を中断してコマンド待ち状態に戻る（S 1 3）。

【 0 0 4 0 】

そうでない場合は、次のステップ S 6 に進む。S 6 において、C P U 5 8 は暗号化されたマスタ I D 用共通鍵 1 0 1 a により暗号化解除する。そして平文化されたマスタ I D（16 ビット）を取得する。

次に S 7 において、C P U 5 8 は磁気ヘッド 1 4 をメディア個別 I D 情報が格納されているトラックへシークさせる。

30

【 0 0 4 1 】

さらに S 8 において、本トラックに記録された I D 情報の読出しが実行され、メディア個別 I D 情報を含むセクタデータがバッファメモリ 6 3 に読み込まれる。

S 9 において、C P U 5 8 はまず、セクタデータ内のデジタル署名データをメディア個別 I D 用公開鍵 1 0 1 d を用いて暗号化解除する。次に所定のハッシュ関数によりセクタデータ内のメディア個別 I D のデータのハッシュコードを計算する。ここで所定のハッシュ関数は図 9 の I D 情報記録装置におけるハッシュ関数演算器 7 3 に適用される関数と同一の関数となっている。

【 0 0 4 2 】

40

次に S 9 において、C P U 5 8 は前ステップにおけるデジタル署名を暗号化解除したコードと、メディア個別 I D から計算したハッシュコードを比較する。ここでもしこれらが異なっていた場合は、メディアに何らかの異常があると判断し、S 1 4 で上位装置へ異常の発生を通知する。そして処理を中断してコマンド待ち状態に戻る。

【 0 0 4 3 】

そうでない場合は、次のステップ S 1 1 に進む。S 1 1 において、C P U 5 8 は暗号化されたメディア個別 I D をメディア個別 I D 用共通鍵 1 0 1 c により暗号化解除する。そして平文化されたメディア個別 I D（32 ビット）を取得する。最後に S 1 2 において、C P U 5 8 はマスタ I D（16 ビット）とメディア個別 I D（32 ビット）を結合し、48 ビットの I D を作成する。そしてこれをバス 6 2 を介して上位装置 6 1 に送る。そしてそ

50

の後、S 1 3 で上位装置 6 1 からのコマンド待ち状態に戻る。

【0044】

上位装置 6 1 はその後必要に応じて、その他のヘッドに対しても同様に I D の読出しコマンドを送る。そして各ヘッドに対応する I D を取得し、これらを元に暗号鍵の生成等を行う。

【0045】

【発明の効果】

以上説明したように本発明の磁気ディスク媒体によれば、メディアを一意に識別するための I D 情報を、プリエンボス型磁気ディスクのプリフォーマット領域と、非プリフォーマット領域とに分けて記録するようにしたため、改竄が困難であると共に一意性の有る I D 10 情報を記録した磁気ディスク媒体を提供可能となる。

【0046】

また、本発明の固定磁気ディスク装置によれば、上記磁気ディスク媒体を 1 枚以上内蔵し、本磁気ディスク媒体から I D 情報を読み出して上位装置に転送することができるため、様々なセキュリティシステムに適用可能な固定磁気ディスク装置を提供可能となる。

【図面の簡単な説明】

【図 1】本発明の実施形態の磁気ディスクの初期磁化の原理説明図で、(a) は一次着磁を示し、(b) は二次着磁を示す。

【図 2】本発明の実施形態の磁気ディスクの平面図 (その 1) である。

【図 3】本発明の実施形態の磁気ディスクの平面図 (その 2) である。 20

【図 4】本発明の実施形態の磁気ディスクの製造方法の説明図である。

【図 5】本発明の実施形態の固定磁気ディスク装置の構成図である。

【図 6】本発明の実施形態の磁気ディスクの記録面の詳細図である。

【図 7】本発明の実施形態の磁気ディスクの製造に用いるスタンプの製造装置の説明図である。

【図 8】本発明の実施形態の固定磁気ディスク装置の制御部の構成図である。

【図 9】本発明の実施形態の磁気ディスクのメディア個別情報の書き込み装置の構成図である。

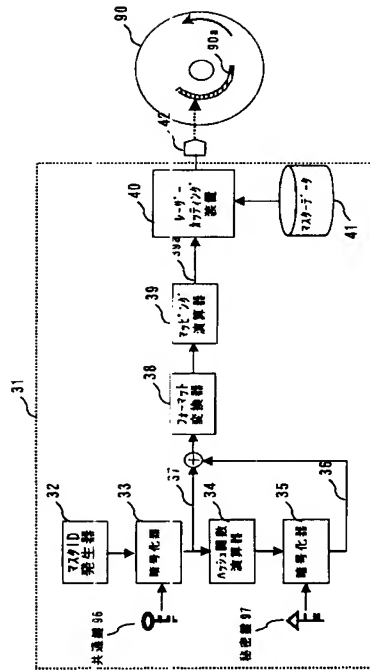
【図 10】本発明の実施形態の固定磁気ディスク装置において磁気ディスクに格納された I D 情報を読み出す手順を示すフローチャートである。 30

【図 11】本発明の実施形態の固定磁気ディスク装置に保管する鍵テーブルの内容を示す図である。

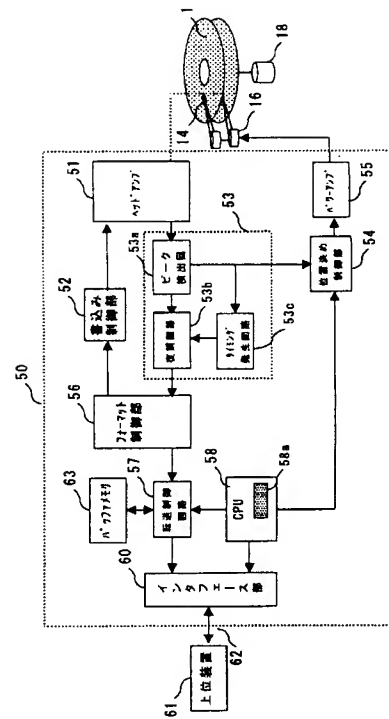
【符号の説明】

- 1 磁気ディスク
- 2 サーボゾーン
- 3 マスタ I D 情報
- 4 メディア個別 I D 情報

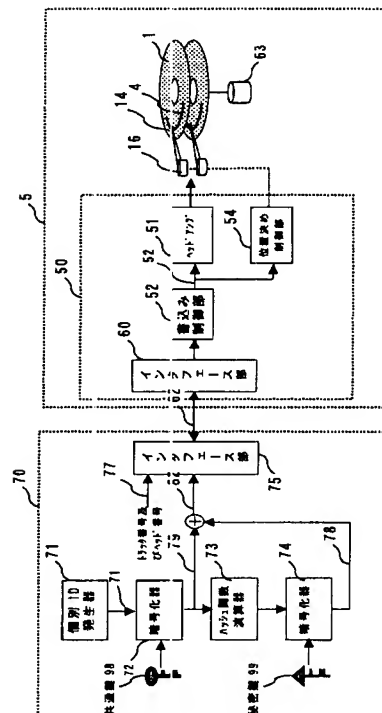
【图 7】



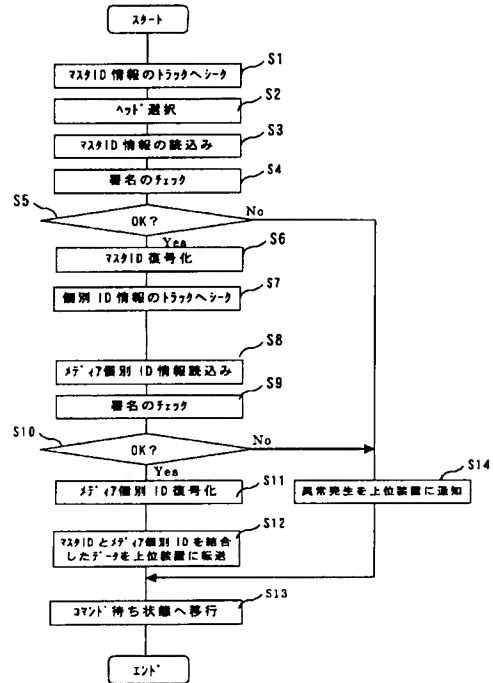
【图 8】



【 図 9 】



【 ㊦ 1 0 】



【図 11】

101

No.	内容	
1	マスタ ID 用共通鍵	101a
2	マスタ ID 用公開鍵	101b
3	メディア個別 ID 用共通鍵	101c
4	メディア個別 ID 用公開鍵	101d